February 24, 2006

Information Technology Management

Select Controls for the Information Security of the Ground-Based Midcourse Defense Communications Network
(D-2006-053)

Department of Defense
Office of Inspector General

Quality   *Integrity*   *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **24 FEB 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: Select Controls for the Information Security of the Ground-Based Midcourse Defense Communications Network	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ODIG-AUD (ATTN: AFTS Audit Suggestions),Inspector General of the Department of Defense,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Acronyms

CIO	Chief Information Officer
GAO	Government Accountability Office
GCN	GMD Communications Network
GMD	Ground-Based Midcourse Defense
IA	Information Assurance
MAC	Mission Assurance Category
MDA	Missile Defense Agency
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SSAA	System Security Authorization Agreement

February 24, 2006

MEMORANDUM FOR DIRECTOR, MISSILE DEFENSE AGENCY
CHIEF INFORMATION OFFICER, MISSILE
DEFENSE AGENCY

SUBJECT: Report on Select Controls for the Information Security of the
Ground-Based Midcourse Defense Communications Network (Report
No. D-2006-053)

We are providing this report for review and comment. We considered
management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly.
The comments of the Deputy Director, Missile Defense Agency, responding for the
Director, Missile Defense Agency, were partially responsive or nonresponsive to some of
the recommendations. As a result of management comments, we revised
Recommendation 1. Therefore, we request that the Director, Missile Defense Agency,
provide additional comments on those recommendations by March 24, 2006.

If possible, please send management comments in electronic format (Adobe
Acrobat file only) to AudRLS@dodig.osd.mil. Copies of the management comments
must contain the actual signature of the authorizing official. We cannot accept the
/ Signed / symbol in place of the actual signature. If you arrange to send classified
comments electronically, they must be sent over the SECRET Internet Protocol Router
Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to
Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Ms. Karen J. Lamar at (703)
604-9005 (DSN 664-9005). See Appendix C for the report distribution. The team members
are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Wanda A. Scott
Assistant Inspector General
Readiness and Logistic Support

Department of Defense Office of Inspector General

Report No. D-2006-053   **February 24, 2006**
  (Project No. D2005-D000AL-0152)

Select Controls for the Information Security of the Ground-Based Midcourse Defense Communications Network

Executive Summary

Who Should Read This Report and Why? The Director and Chief Information Officer, Missile Defense Agency, and other Missile Defense Agency managers responsible for making operational and information assurance-related decisions pertaining to the Ground-Based Midcourse Defense Communications Network should read this report to reduce the risk of interruption, misuse, modification, and unauthorized access to information in the system. Additionally, all DoD Component Chief Information Officers with oversight responsibilities for contractor-owned or operated systems should read this report.

Background. This report is one in a series on operational control reviews at the Missile Defense Agency. In May 2003, the President directed DoD to field an initial set of missile defense capabilities and begin operating them in 2004 and 2005. In recent years, more countries are developing sophisticated missiles that are capable of reaching the United States. Ballistic missile defense is a challenging mission because of the speed and altitude of a ballistic missile. In late 2004, the United States fielded the initial Ballistic Missile Defense System that can be used for limited defense operations. The Ballistic Missile Defense System is comprised of various elements to include the Ground-Based Midcourse Defense system, which is contractor-owned and operated. The system includes infrastructure, sensors, radars, and interceptors, which are connected by the Ground-Based Midcourse Defense Communications Network. This network provides connectivity for all system components to transfer and process information to operators performing engagement activities.

DoD Component Heads are required to establish minimum information assurance controls outlined in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, for all systems in order to protect the integrity, availability, and confidentiality of the information in that system. The Missile Defense Agency Chief Information Officer established the Ground-Based Midcourse Defense Communications Network's baseline of required information assurance controls as the most stringent for integrity, availability, and confidentiality.

DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, requires that DoD Component and DoD contractor information technology systems and networks undergo a formal certification and accreditation process to authorize systems to operate. During the DoD Information Technology Security Certification and Accreditation Process, the information assurance controls of DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, are implemented. The certification and accreditation process culminates in a decision to grant a system an authority to operate, an interim authority to operate, or no authority to operate.

Results. Missile Defense Agency officials had not prepared a System Security Authorization Agreement for the Ground-Based Midcourse Defense Communications Network. Additionally,

available security documentation did not properly reflect current operations of the network. Missile Defense Agency officials also had not fully implemented information assurance controls required to protect the integrity, availability, and confidentiality of information in the Ground-Based Midcourse Defense Communications Network. Specifically, the Missile Defense Agency program office for the Ground-Based Midcourse Defense Communications Network did not provide information assurance awareness training to prior to being granted access, conduct reviews for unauthorized access, properly implement or document user access procedures and controls, and prepare contingency and incident response plans. Further, a Plan of Action and Milestones designed to assist managers in correcting security weaknesses had not been prepared. As a result, Missile Defense Agency officials may not be able to reduce the risk and extent of harm resulting from misuse or unauthorized access to or modification of information of the Ground-Based Midcourse Defense Communications Network and ensure the continuity of the network in the event of a disruption. Additionally, the Missile Defense Agency Chief Information Officer and the Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the Ground-Based Midcourse Defense Communications Network if required key documents are not prepared, updated, or tested. See the Finding section of the report for the detailed recommendations.

Management Comments. The comments of the Deputy Director, Missile Defense Agency, responding for the Director, Missile Defense Agency, were partially responsive or nonresponsive to some of the recommendations. See the Finding section of the report for a discussion of management comments on the recommendations and the Management Comments section of the report for the complete text of the comments.

We request that the Director, Missile Defense Agency comment on this report by March 24, 2006.

Table of Contents

Background

In May 2003, the President directed DoD to field an initial set of missile defense capabilities and begin operating them in 2004 and 2005. The mission of the Missile Defense Agency (MDA) is to develop an integrated Ballistic Missile Defense System to defend the United States, its deployed forces, and allies from ballistic missiles. In recent years, more countries are developing sophisticated missiles that are capable of reaching the United States. Ballistic missile defense is a challenging mission because of the speed and altitude of a ballistic missile.

In late 2004, the United States fielded the initial Ballistic Missile Defense System that can be used for limited defense operations. The Ballistic Missile Defense System is comprised of various elements to include the Ground-Based Midcourse Defense (GMD) system. The GMD system consists of the following components:

- GMD Communications Network (GCN);

- Command Launch Equipment, Fire Control Communications, Ground Based Support, and In-Flight Interceptor Communications Systems; and

- sensors, radars, and interceptors.

The GCN provides connectivity for all GMD components in order to transfer and process information to operators performing engagement activities. The MDA Program Office for GMD is responsible for the information assurance (IA) and the certification and accreditation of all components of the GMD system.

GMD Communications Network. The GCN, a contractor-owned and operated system, has two main components—encrypted and unencrypted equipment—both comprised of a communications and a monitoring system. The communications systems receive information from the various sensors and radars and transmits that information to the various components of GMD. The monitoring systems report on the health and status of the communications systems. The GCN has been in development since January 2001.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requires that all DoD information systems maintain an appropriate level of IA by establishing a baseline of controls for integrity, availability, and confidentiality. The DoD Component Head is required to designate a Mission Assurance Category (MAC)[1] level for all systems in order to determine those minimum IA controls identified in DoD Instruction 8500.2 to protect the integrity and availability of the information in that system. The MDA Chief Information Officer (CIO) designated the GCN as a MAC I system in the DoD Information Technology

---

[1] A MAC level is identified for all DoD information systems and reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MAC I systems are those that require the most stringent DoD Instruction 8500.2 controls for integrity and availability.

Registry.[2] For MAC I systems, the IA controls for integrity and availability are always the most stringent. The confidentiality level for MAC I systems is determined by whether the system processes classified, sensitive, or public information. MDA Policy Memorandum, "Designated Approving Authority (DAA) Accreditation Directions to Ballistic Missile Defense System (BMDS) Elements for Mission Automated Information Systems," April 13, 2004, mandated that Ballistic Missile Defense System mission systems and elements implement the classified IA controls identified in DoD Instruction 8500.2. The baseline of IA controls for the GCN is the most stringent for integrity, availability, and confidentiality.

Certification and Accreditation Process. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, requires that DoD Component and DoD contractor information technology systems and networks establish a formal certification and accreditation process to authorize systems to operate. DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process," July 31, 2000, standardizes the certification and accreditation process throughout DoD. During the DoD Information Technology Security Certification and Accreditation Process, the IA controls of DoD Instruction 8500.2 are implemented. A Systems Security Authorization Agreement (SSAA) documents the actions, decisions, IA requirements, and the level of effort needed to certify and accredit any information system. The DoD Information Technology Security Certification and Accreditation Process is composed of activities and tasks designed to protect information systems and networks from loss, alteration of, denial of access to, or unauthorized access to system information. The certification and accreditation process culminates in a decision to grant a system an authority to operate, an interim authority to operate,[3] or no authority to operate. In March 2005, the MDA Designated Approving Authority granted the GCN a six month interim authority to operate and, in August 2005, renewed that interim authority to operate for an additional six months.

Objectives

The overall audit objective was to determine whether information security operational controls operate effectively and provide an appropriate level of IA. Specifically, the audit assessed the adequacy and effectiveness of the security program, access controls, and contingency and continuity of operations plans. We also evaluated the management control program related to the objective. This report addresses the GCN and is one in a series on information security reviews at MDA. See Appendix A for a discussion of the audit scope and methodology.

---

[2]The Information Technology Registry is the official database for the DoD-wide inventory of mission critical, mission essential, and select mission support systems. That Registry contains security status for such things as accreditation, risk management, security, incident response, contingency plans, and security testing.

[3]An interim authority to operate is issued when a system does not meet the system security requirements but the mission criticality mandates that it become operational.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We performed tests of the Management Control Program by performing the procedures used to accomplish our objective. The objective was to assess the adequacy and effectiveness of the security program, access controls, and contingency and continuity of operations plans. By performing the procedures to review those controls, in effect, we tested the Management Control Program for those select operational controls.

Adequacy of Management Controls. We found weaknesses in the Management Control Program for the security program, access controls, and contingency and continuity of operations plans. For specific results of those weaknesses, see the Finding section of the report. The recommendations, if implemented, will correct the identified weaknesses. A copy of the report will be provided to the senior official responsible for management controls at MDA.

Adequacy of Management's Self-Evaluation. We found weaknesses in management's self-evaluation processes for implementing IA controls for the GCN. MDA reviewed the adequacy of management controls by performing financial, operational, compliance, and program reviews and audits; however, they performed no IA reviews of their information systems. Additionally, the MDA CIO did not identify any reportable material weaknesses and assured in his management control assessment that information technology was adequately protected.

Ground-Based Midcourse Defense Communications Network Information Security Status

MDA officials had not prepared an SSAA for the GCN. Additionally, available security documentation did not properly reflect current operations of the network. MDA officials also had not fully implemented select IA controls required to protect the integrity, availability, and confidentiality of GCN information. Specifically, the MDA program office for the GCN did not:

- provide IA awareness training to GCN users prior to being granted access to the GCN;

- conduct reviews for unauthorized access;

- properly implement or document user access procedures and controls; and

- prepare contingency and incident response plans.

Further, a Plan of Action and Milestones (POA&M) designed to assist managers in correcting security weaknesses was not prepared. MDA officials did not prepare required documents and implement IA controls because they did not conduct adequate oversight of the GCN IA program, update the development contract to adhere to DoD policy, or assign IA roles and responsibilities for the GCN development process. As a result, MDA officials may not be able to reduce the risk and magnitude of harm resulting from misuse or unauthorized access to or modification of information of the GCN and ensure the continuity of the system in the event of a disruption. Additionally, the MDA CIO and the Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the GCN if required key documents are not prepared, updated, or tested.

System Security Authorization Agreement

MDA officials had not prepared an SSAA for the GCN. Additionally, available security documentation did not properly reflect current operations of the network.

System Security Authorization Agreement. The DoD Information Technology Security Certification and Accreditation Process uses a single document approach—the SSAA—for the certification and accreditation process. The SSAA is designed to fulfill the requirements of Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 2000, for a security plan and to meet all Federal, DoD, and MDA requirements for documentation of system and network certification and accreditation. The SSAA is used throughout the

DoD Information Technology Security Certification and Accreditation Process to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security. The DoD Information Technology Security Certification and Accreditation Process applies to all systems requiring certification and accreditation throughout their life cycle. The process is designed to adapt to any type of information system and any computing environment and mission. Contractor officials prepared, and MDA officials authorized, four individual SSAAs for the various components of GCN and granted interim authorities to operate based on each of those SSAAs. Contractor officials stated that they no longer grant multiple interim authorities to operate based upon the components of GCN, but on GCN as a whole. Therefore, because GCN was granted one interim authority to operate, which is the result of the DoD Information Technology Security Certification and Accreditation Process, it requires an SSAA. However, officials did not prepare a GCN SSAA. MDA officials should prepare an overall SSAA for GCN because the SSAA contains the documentation to support the interim authority to operate and applies to all systems that require certification and accreditation.

Available Security Documentation. MDA officials did not prepare and update the various GCN component SSAAs to adequately reflect the current operating system mission, environment, and architecture. Specifically, contractor officials had not prepared key documents required by OMB Circular A-130 to support the individual GCN component SSAAs and did not report valid or current information in those SSAAs. For instance, contingency plans and system rules of behavior had not been prepared to assist users. Additionally, the SSAA for the unencrypted communications system stated that an individual password was required; however, the developing contractor used group passwords. The SSAAs for the unencrypted equipment also identified a security concept[4] for the unencrypted equipment; however, that concept covered encrypted equipment instead of unencrypted equipment. On the other hand, SSAAs for the encrypted equipment did not contain any security concept. This oversight occurred because the encrypted equipment and the unencrypted equipment were developed by two separate contractors, who were not following a common set of procedures for preparing documentation.[5]

User Representative. The key to the DoD Information Technology Security Certification and Accreditation Process is the agreement between the designated approving authority, the certifying authority, the program manager, and the user representative. Those individuals resolve schedule, budget, security, functionality, and performance issues. A user representative is responsible for ensuring that the system meets the user's operational need, meets the availability and integrity requirements, and has a realistic security policy that can be maintained in the operational environment. The GMD Deputy Designated Approving Authority stated that the Joint Functional Component Command was the user of the GCN; however, the GCN component SSAAs identified U.S. Northern Command as the user representative. However, no user representative had endorsed those SSAAs to ensure

---

[4]The purpose of the security concept was to provide a description of the GCN security requirements and resources needed to meet those requirements.

[5] Boeing is the prime contractor for the development of the GMD system, which includes the GCN. Northrop Grumman is a sub-contractor to Boeing and develops all the unencrypted equipment for the GMD system, which includes the unencrypted equipment for the GCN.

that the needs of the user were being met. According to the GMD Deputy Designated Approving Authority, the GCN has multiple users; therefore, ongoing efforts are trying to determine who the user representative should be. MDA officials should identify the user representative to ensure that the GCN is being developed to meet the operational needs of that user.

Information Assurance Controls

MDA officials had not fully implemented select IA controls required to protect the integrity, availability, and confidentiality of the GCN information. The GCN, a contractor-owned and operated system, is reported in the Information Technology Registry as a MAC I system. According to MDA Policy Memorandum, "Mission Assurance Category (MAC) Levels for Missile Defense Agency (MDA) Systems and Networks," August 20, 2004, all MDA systems are required to be accredited in accordance with DoD Instruction 8500.2. However, GMD government program and contractor officials did not develop the GCN to meet DoD Instruction 8500.2 requirements. Rather, they developed the GCN to conform to the standards of DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 26, 1985, which does not include most of the IA controls required in DoD Instruction 8500.2. Further, based on a cross-walk provided by the independent assessment team contracted to perform the independent verification and validation function for GMD, the IA controls actually being implemented were those from DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988. In any event, the IA controls required by DoD 5200.28-STD and DoD Directive 5200.28 were outdated and did not comply with the current IA controls identified in DoD Instruction 8500.2, such as IA awareness training, intrusion detection, real-time monitoring, and contingency planning. MDA officials should immediately implement all IA controls of DoD Instruction 8500.2 for the GMD element.

Information Assurance Awareness Training. DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, requires that all authorized users, including contractors, receive IA awareness training as a condition for access to any DoD system and, thereafter, complete annual IA refresher training. Contractor personnel who had access to the GCN did not receive IA awareness training prior to being granted access to the system. In April 2005, MDA officials implemented the IA awareness training requirement for the first time; by October 2005, all GCN contractor personnel had completed the training. MDA program officials for GMD stated that they had not required the IA awareness training until MDA implemented the IA awareness training requirement. MDA officials should continue to promote awareness and provide recurring training to all employees and contractors so that all government and contractor personnel are aware of their security roles and responsibilities and understand current government policies and procedures, security risks, and the potential threats to MDA systems.

User Access Controls. MDA and contractor officials did not conduct adequate reviews for potential acts of unauthorized access into the GCN, implement consistent

password procedures, or implement procedures to ensure that access was granted to only those users with the required clearance and who had received IA awareness training.

Unauthorized Access Review. MDA and contractor officials did not conduct audit log reviews for the unencrypted communications and monitoring systems of the GCN. MDA and contracting officials stated that audit log reviews were only required for the encrypted communications and monitoring systems and that those reviews were performed manually. Contractor officials also stated that manual audit log reviews were cumbersome and time-consuming and that those reviews did not guarantee the detection of all relevant security violations. However, DoD Instruction 8500.2 requires the deployment of an automated, continuous on-line monitoring and audit trail capability to immediately alert personnel to any unusual or inappropriate activity with potential IA implications. Contractor officials stated that they did not implement real-time audit log monitoring capability on the GCN system because it was not in the contract. Both government and contractor officials acknowledged that automated audit log monitoring systems would be beneficial to the GCN system because predefined events could be established to identify security trends and patterns of unauthorized access. MDA and contractor officials should integrate an automated monitoring capability into the GCN in order to alert the appropriate personnel of a security incident for the GCN system. MDA and contractor officials should also conduct weekly manual reviews of the audit logs for all GCN components until such time that an automated monitoring capability is installed into the system.

User Account Management. DoD Instruction 8500.2 requires that users gain access to DoD information systems with the use of an individual identifier and password. Officials did not require users to have an individual password to access the unencrypted communications system of the GCN. Contractor officials explained that based on the configuration of the GCN, an individual password was not necessary to protect against unauthorized use. Specifically, a group password was used to authenticate a user of the unencrypted communications system. However, access to that communications system could only be gained via the unencrypted monitoring system, which required an individual password to access that monitoring system. Contractor officials stated that plans were underway to configure the unencrypted communications system to have role-based passwords, which assigns the same password to a group of users with the same level of access to the system. An MDA official stated that the reconfiguration to the passwords will not be implemented until March 2006. DoD policy does not allow for individual or role-based passwords, even when the configuration of the system provides protection against unauthorized access. It is especially important that MDA officials implement consistent password controls that comply with DoD Instruction 8500.2 because, according to those officials, the greatest risk to the GCN system was the insider threat.

DoD Instruction 8500.2 also requires the implementation of a comprehensive account management process to ensure that only authorized users gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. Contractor officials did not implement a plan or prepare procedures to promptly deactivate inactive, suspended, or terminated accounts. Contractor

officials stated that no user had an inactive, suspended, or terminated account as of July 2005; therefore, the contractor did not believe they needed to implement procedures for the deactivation of accounts. However, in November 2005, contracting officials terminated two unnecessary accounts for users who no longer required access to the GCN. MDA officials should require the contractor to immediately prepare and implement account management procedures to include deactivation of inactive, suspended, or terminated accounts.

User Account Request Forms. DoD Instruction 8500.2 requires that the IA Officer ensure that users have the requisite security clearances and supervisory need-to-know authorization and are made aware of their IA responsibilities before being granted access to any DoD information system. However, the initial GCN IA Officer[6] was not appointed until June 2005, almost a year after the GCN became operational.[7] The procedures used by contractor officials to control and grant access to the GCN required that the user complete an account request form that included the:

- user request for access;

- type of user access being requested;

- supervisor approval and signature that the user had a valid "need-to-know;" and

- GCN security manager certification that the user had the requisite security clearance needed for the system.

We reviewed the user account request forms for all GCN users. As of July 2005, there were 22 user accounts for the GCN. The GCN security manager had not signed any of those forms verifying that a user had the required security clearance for the GCN until July 2005, approximately one year after the GCN became operational. Additionally, contractors processing those user account request forms stated that they did not include the actual date a user was granted access to the GCN; instead, the contractors used the date the user completed the form. Additionally, the GCN procedures used to control and grant access to the encrypted communications and monitoring systems did not require that the user account request form require the IA Officer to certify that a user had received IA awareness training prior to being granted access to the GCN. Also, procedures to control and grant access to the unencrypted systems were not prepared. Contractor officials stated they would update the user account request form to include a section for the IA Officer to certify in writing that he or she had, in fact, verified the user's completion of the IA awareness training.

In November 2005, contractor officials implemented the revised user account request form and required GCN users to complete that form. However, we identified problems with the content and completion of the revised forms. First, the system administrator responsible for creating accounts on the GCN

---

[6]The IA Officers appointed for the GCN are contractor employees of MDA.

[7]In late 2004, the U.S. fielded an initial Ballistic Missile Defense System that can be used for limited defense operations.

created his own account and granted himself all special access requirements allowed for the GCN; however, we could not determine whether those access requirements were appropriate. Second, the revised forms were not completed by the unencrypted communications and monitoring systems users. Third, the IA Officer and security manager at one operating location certified IA training requirements and security clearances on the user account access forms for a location they were not responsible for. Fourth, two accounts were still active when those users were no longer at that operating location. Lastly, the security manager certified users' clearances a day after our receipt of the revised forms. MDA officials should require the contractor to update and prepare procedures that require the user account request form to include the date users are granted initial access to the system in order to track that annual IA refresher training is provided and require the IA Officer to certify by initialing the form that the:

- user completed the IA awareness training;

- supervisor verified the user's role and need-to-know; and

- security manager certified that the user holds a valid and appropriate clearance.

MDA officials should also reconcile all active user accounts by operating location to ensure that access is still required. Additionally, MDA officials should revise the user account request form to include the initial date a user was granted access to the GCN and include a section on the form for the IA Officer to initial that the form contains all required signatures and is complete and accurate. Further, MDA officials should review all user accounts to ensure each user was granted the appropriate level of access and ensure that no user can authorize their own account in the system without validation by an independent party that the access requirements granted were appropriate.

Contingency and Incident Response Planning. GMD officials did not implement the DoD Instruction 8500.2 IA controls for contingency and incident response planning.

  Contingency Plan. DoD Instruction 8500.2 requires preparation of a disaster plan that provides for the smooth transfer of all mission and business-essential functions to an alternate site with little or no loss of operational continuity. A system's contingency plan may be included as part of the system's disaster recovery procedures. GMD officials stated that they had not prepared a formal contingency plan for the GCN because redundant operations were built into the configuration of the system that would mitigate most interruptions. DoD Instruction 8500.2 requires formal documentation of the essential functions for priority restoration, the identification of an alternate location that permits the restoration of those essential functions, and implementation of recovery procedures to ensure recovery is done in a secure and verifiable manner. Regardless that the design of the GCN may reduce most interruptions, GMD officials should document those procedures and operations that will prevent the GCN from potential loss of information or operations should an incident occur.

Incident Response Plan. Contractor officials did not prepare a formal incident response plan for the GCN system. Contractor officials stated that they report on equipment and communications outages; however, they do not have a formal plan to report security incidents or violations. DoD Instruction 8500.2 requires that an incident response plan exist that identifies the responsible computer network defense service provider, defines reportable incidents, outlines a standard operating procedure for incident response, provides for user training, and establishes an incident response team. MDA officials should require the contractor to implement a formal incident response plan to ensure employees are made aware of the incident response procedures to alert the appropriate parties if an incident occurs.

Plan of Action and Milestones

MDA officials did not implement a formal plan that would assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses identified for the GCN, which operated under an interim authority to operate. According to DoD 8510.1-M, an interim authority to operate is issued when the system does not meet the system security requirements but the mission criticality mandates that it become operational. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2005 (FY05)," April 18, 2005, required that DoD Components prepare and submit a POA&M that identifies the solution, schedule, security actions, and milestones necessary for mitigating identified security weaknesses. It is especially important to prepare a POA&M for systems operating under an interim authority to operate.

Although contractor officials routinely assessed the GCN to identify IA security weaknesses, the developing contractor and the independent assessment team contractor maintained the results of those assessments separately. The MDA program office for GMD did not prepare a POA&M that readily identified the weaknesses, the tasks and resources needed to mitigate the weaknesses, the milestones, and scheduled completion dates for the milestones. Although aspects of a POA&M were maintained separately and weaknesses tracked through mitigation schedules, the information was not maintained centrally by the MDA program office for GMD. Subsequent to our review, MDA officials consolidated the IA weaknesses of the developing contractor and the independent assessment team contractor, and in September 2005, provided a plan that met the requirements of a POA&M. MDA officials should conduct quarterly reviews and updates of the POA&M in order to measure and monitor the progress of efforts needed to mitigate the security weaknesses identified for the GCN, including all weaknesses identified by this audit. We commend management for taking initial corrective action on this issue.

Management Controls

MDA officials did not implement IA controls and prepare required documents because they did not conduct adequate oversight of the GCN IA program, update the development contract to adhere to DoD policy, or assign IA roles and responsibilities for the GCN development process.

Contractor officials stated that because the GCN had been in development for approximately five years, it would have been too costly to modify the development contract to implement the IA controls required in DoD Instruction 8500.2; however, security requirements cannot simply be waived based on cost. MDA Policy Memorandum, "Mission Assurance Category (MAC) Levels for Missile Defense Agency (MDA) Systems and Networks," August 20, 2004, required that MDA systems and networks not accredited in accordance with DoD Instruction 8500.2 be approved in writing from the MDA Designated Approving Authority; however, no written approval was obtained. Additionally, the MDA CIO stated that although the contractor had not implemented all the IA controls required by DoD Instruction 8500.2, the standards used, DoD 5200.28-STD, met approximately 85 percent of those IA controls. However, that standard is twenty years old and does not include requirements for the current IA controls of DoD Instruction 8500.2. Also, the GCN program office was not involved in the preparation of the available security documentation.

MDA officials had not prepared IA policies for incident response and recovery, passwords, configuration change, IA training, and audit management. MDA officials only first entered into a contract for the development of those IA policies in June 2005, after an assessment of their IA program conducted by the National Security Agency. GMD program and contractor officials stated that at the time, IA had not been emphasized by MDA and that they were not aware of their IA responsibilities. Additionally, an IA Manager[8] responsible for oversight of the GMD system's IA program was not appointed until July 2005 and the IA Officers were not appointed until the last six months of the five year development of the GCN.

Conclusion

MDA and contractor officials may not be able to reduce the risk and magnitude of harm resulting from misuse or unauthorized access to or modification of the information of the GCN, and ensure the continuity of the system in the event of an interruption. Additionally, the MDA CIO and Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the GCN if contingency and incident response plans are not prepared or tested and the system security plan is not prepared and updated on a recurring basis. MDA and contractor officials must immediately comply with all Federal, DoD, and MDA

---

[8]The IA Manager, an MDA government employee, is responsible for developing and maintaining the GMD IA program to include identifying the IA objectives and policies, ensure the development and maintenance of IA certification documents, maintain a repository of IA certification and accreditation documents, ensure that IA Officers are appointed in writing and provide oversight to ensure that they are following IA policies, and ensure that IA Officers receive necessary IA training.

system security requirements for GCN, emphasize the importance of IA to MDA and contractor employees, conduct timely IA awareness training of GCN users, conduct reviews of unauthorized access, and implement password procedures and controls for user access so that the confidentiality, integrity, and availability of the information in the GCN is not compromised and is protected to the highest level possible.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. We revised Recommendation 1. to request that MDA identify the primary user representative for the GCN, rather than for the GMD, so that the GCN meets the user's operational need.

We recommend that the Director, Missile Defense Agency ensure that the Chief Information Officer, Missile Defense Agency:

1. Completes the System Security Authorization Agreement process for the Ground-Based Midcourse Defense Communications Network in full compliance with Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 30, 2000, and DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000, by April 1, 2006 and identify the primary user representative for the Ground-Based Midcourse Defense Communications Network to ensure that the network will meet the user's operational need; will meet the availability and integrity requirements; and has a realistic security policy that can be maintained in the operational environment.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred that a single SSAA would be prepared for the GCN, stating that the single SSAA would be staffed for signature with the GMD Program Director. However, the Deputy Director nonconcurred with identifying the primary user representative for the GCN stating that a user representative had authorized the GMD and the Ballistic Missile Defense System SSAAs.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were partially responsive. We revised this recommendation and request that MDA identify the primary user representative for the GCN, rather than for the GMD, so that the GCN meets the user's operational need.

2. Immediately implements all information assurance controls required in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, for Mission Assurance Category I and classified systems. Specifically,

a. Prepare and implement procedures for the Ground-Based Midcourse Defense Communications Network to:

(1) Deactivate inactive, suspended, and terminated accounts.

(2) Mandate that the information assurance officer track the date a user is granted access to the system, certify the user completed information assurance awareness training, and verify that the user has a valid and appropriate security clearance.

(3) Require that an independent party validate in the Ground-Based Midcourse Defense Communications Network that access requirements granted were appropriate when a user creates their own account.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that the prime contractor implemented the process to deactivate inactive, suspended, and terminated accounts and that since the establishment of the IA Officers, a common process and forms for granting access was developed, audited, and verified.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were responsive to the recommendation; therefore, no further comments are required.

b. Update the Ground-Based Midcourse Defense Communications Network configuration to include:

(1) Automated monitoring of the unencrypted and encrypted communications and monitoring systems; and

(2) Individual user passwords to access the unencrypted communications system.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that current equipment is not capable of performing automated audit log assessment. Until that capability is available manual reviews are conducted weekly. Additionally, the Deputy Director stated that shared passwords have been eliminated with the release of the 4B.1 software build. However, on February 1, 2006, a contracting official stated that the 4B.1 software build would not be released until May 2006.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were nonresponsive. The Deputy Director did not state whether the automated audit log capability would be implemented on the GCN. While we acknowledge that management has implemented the requirement for weekly manual reviews, management must ensure that an automated audit log capability is implemented in the system. Additionally, as stated in this report, plans were underway to configure the unencrypted communications system during the 4B.1 software build to have role-based passwords, which would assign the same password to a group of users with the same level of access to the system, rather than individual passwords. However, DoD policy does not allow for individual or role-based passwords. Further, management comments were inconsistent as to when the 4B.1 software build would be implemented. We request that management provide additional comments to identify when

individual passwords, not role-based passwords, would be implemented for the unencrypted communications system of the GCN.

c. Prepare a contingency plan for the Ground-Based Midcourse Defense Communications Network that meets the requirements of DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that a pending engineer change proposal statement of work will address the IA requirements. The Deputy Director also stated that contingency plans were present at each site.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were partially responsive. Although the Deputy Director stated that plans were underway to prepare a contingency plan, he did not state whether it would be prepared in accordance with DoD Instruction 8500.2 and National Institute of Standards and Technology Special Publication 800-34. Additionally, MDA and contracting officials at the sites told the audit team that there were no contingency plans in place. We request that management provide additional comments to identify whether the contingency plan will be prepared in accordance with DoD Instruction 8500.2 and National Institute of Standards and Technology Special Publication 800-34.

d. Prepare an incident response plan for the Ground-Based Midcourse Defense Communications Network that meets the requirements of DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and the National Institute of Standards and Technology Special Publication 800-61, "Computer Security Incident Handling Guide," January 2004.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that a pending engineer change proposal statement of work will address the IA requirements. The Deputy Director also stated that incident response plans were present at each site.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were partially responsive. Although the Deputy Director stated that plans were underway to prepare an incident response plan, he did not state whether it would be prepared in accordance with DoD Instruction 8500.2 and National Institute of Standards and Technology Special Publication 800-61. Additionally, MDA and contracting officials at the sites told the audit team that there were no incident response plans in place. We request that management provide additional comments to identify whether the incident response plan will be prepared in accordance with DoD Instruction 8500.2 and National Institute of Standards and Technology Special Publication 800-61.

3. Maintains the information assurance training program for all Missile Defense Agency and contractor personnel associated with the Ground-Based

Midcourse Defense Communications Network in accordance with DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that the training process is uniform across all the components and contractors.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were responsive to the recommendation; therefore, no further comments are required.

4. Updates the Plan of Action and Milestones to include all security weaknesses identified for the Ground-Based Midcourse Defense Communications Network, including all weaknesses identified in this review.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that the POA&M will be reviewed quarterly to update and include new actions and milestones, such as the DoD, Office of the Inspector General findings.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were responsive to the recommendation; therefore, no further comments are required.

5. Reports in the Missile Defense Agency's Annual Statement of Assurance the information assurance weaknesses identified in this report for the Ground-Based Midcourse Defense Communications Network.

Management Comments. The Deputy Director, MDA, responding for the Director, MDA, concurred stating that a change to the MDA Annual Statement of Assurance will be considered at the annual update.

Audit Response. The Deputy Director, MDA, responding for the Director, MDA, comments were nonresponsive. We request that management reconsider their position and include all the information assurance weaknesses identified in this report in the MDA Annual Statement of Assurance to ensure full disclosure of system IA weaknesses and management efforts to address those weaknesses.

Appendix A. Scope and Methodology

We queried the DoD Information Technology Registry in March 2005 to identify the MDA information systems designated as mission critical.[*] Each system identified as mission critical was also designated as a MAC I system. We selected the GCN, a mission critical MAC I system, for review. We assessed the adequacy of documentation based on select operational or IA controls designated for the GCN. In DoD guidance, operational controls are included in the definition of IA controls so our report uses the term IA and operational controls interchangeably. We evaluated select IA controls relating to IA awareness training, user access controls, and contingency planning for the GCN system based on the requirements of DoD Instruction 8500.2, DoD 8510.1-M, DoD Directive 8570.1, DoD 5200.28-STD, OMB Memorandum 02-01, OMB Circular A-130, and MDA Policy Memoranda. The policy and guidance reviewed were dated from December 1985 through April 2005.

We reviewed the following GCN documents: the System Security Authorization Agreements, the Interim Authority to Operate Memoranda, appointment letters, IA awareness and role-based training certificates, training plans, audit logs, user account request forms, user access listings, configuration management plans, and risk management plans. We reviewed the relevant documents dated from May 2004 through November 2005.

We visited the GMD Joint Program Office in Huntsville, Alabama, and the Joint National Integration Center, in Colorado Springs, Colorado. Although we did not visit Ft. Greely, Alaska, the GMD Joint Program Office provided the IA policies and procedures (which were the same as the Joint National Integration Center) and the user-specific documents for that location.

We conducted interviews with the MDA CIO, the GMD Deputy Designated Approving Authority, the GMD Certifying Authority, the GMD IA Manager, GMD IA Officers, MDA officials responsible for updating the Information Technology Registry, GCN privileged users, the contractors developing the GCN, and the independent verification and validation contractor team.

We performed this audit from April 2005 to December 2005 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Government Accountability Office High-Risk Area. The Government Accountability Office (GAO) has identified several high-risk areas in DoD. This report provides coverage of the Protecting the Federal Government's Information-Sharing Mechanisms and the Nation's Critical Infrastructures high risk area.

---

[*]Mission Critical systems are those systems that the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations.

Appendix B. Prior Coverage

During the last 5 years, the GAO and the DoD Inspector General (IG) issued 10 reports that discuss the reliability of DoD information technology budget submissions. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD Inspector General reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-05-552, "Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements," July 15, 2005

GAO Report No. GAO-05-381, "DoD Business System Modernization: Billions Being Invested Without Adequate Oversight," April 29, 2005

GAO Report No. GAO-04-858, "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation," July 28, 2004

GAO Report No. GAO-04-823, "Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges," July 21, 2004

GAO Report No. GAO-04-615, "DoD Business System Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability," May 27, 2004

DoD IG

DoD IG Report No. D-2005-099, "Status of Selected DoD Policy on Information Technology Governance," August 19, 2005

DoD IG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005

DoD IG Report No. D-2005-054, "DoD Information Technology Security Certification and Accreditation Process," April 28, 2005

DoD IG Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005

DoD IG Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestone Process," December 13, 2004

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Defense Business Transformation Agency
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Networks and Information Integration/Chief
    Information Officer
Assistant Secretary of Defense for Health Affairs/Chief Information Officer
Assistant Secretary of Defense for Intelligence Oversight/Chief Information Officer
Chief Information Officer, Office of the Secretary of Defense
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff
Chief Information Officer, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Naval Inspector General
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Chief Information Officer, U.S. Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Department of the Air Force

Unified Commands

Chief Information Officer, U.S. Central Command
Chief Information Officer, U.S. European Command
Chief Information Officer, U.S. Joint Forces Command
Chief Information Officer, U.S. Northern Command
Chief Information Officer, U.S. Pacific Command
Chief Information Officer, U.S. Southern Command
Chief Information Officer, U.S. Special Operations Command
Chief Information Officer, U.S. Strategic Command
Chief Information Officer, U.S. Transportation Command

Other Defense Organizations

Director, Missile Defense Agency
Chief Information Officer, American Forces Information Service
Chief Information Officer, Defense Advanced Research Projects Agency
Chief Information Officer, Defense Contract Audit Agency
Chief Information Officer, Defense Contract Management Agency
Chief Information Officer, Defense Commissary Agency
Chief Information Officer, Defense Finance and Accounting Agency
Chief Information Officer, Defense Human Resource Activity
Chief Information Officer, Defense Information Systems Agency
Chief Information Officer, Defense Logistics Agency
Chief Information Officer, Department of Defense Education Activity
Chief Information Officer, Department of Defense Inspector General
Chief Information Officer, Defense Security Cooperation Agency
Chief Information Officer, Defense Security Service
Chief Information Officer, Defense Technical Information Center
Chief Information Officer, Defense Threat Reduction Agency
Chief Information Officer, DoD Test Resources Management Center
Chief Information Officer, Defense Technology Security Administration
Chief Information Officer, Missile Defense Agency
Chief Information Officer, Pentagon Force Protection Agency
Chief Information Officer, TRICARE Management Agency
Chief Information Officer, U.S. Mission North Atlantic Treaty Organization
Chief Information Officer, Washington Headquarters Service

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Missile Defense Agency Comments

DEPARTMENT OF DEFENSE

MISSILE DEFENSE AGENCY
7100 DEFENSE PENTAGON
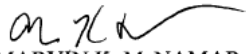WASHINGTON, DC 20301-7100

DO

JAN 2 6 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING,
INSPECTOR GENERAL FOR THE DEPARTMENT OF
DEFENSE

SUBJECT: Response to Draft Report on Select Controls for the Information Security of
the Ground-Based Midcourse Defense Communications Network (Project
No. D2005-D000AL-0152)

     The Department of Defense Inspector General draft report, December 19, 2005,
cited findings from the audit of the Informational Security Operational Controls at the
Missile Defense Agency. The attached documents contain our response to these findings.

     We appreciate the efforts of the review team and generally concur with the draft
findings provided. In most cases the comments provided are to clarify perceptions and
language in the report and to highlight actions already taken to correct the findings.
While we understand the findings report on conditions found during the audit, we are
pleased to report that, in many cases, the findings have since been mitigated or
mitigations are currently underway.

     We very much appreciate the opportunity to review this draft report and to provide
input that we feel is useful to the investigating team. My point of contact for this
submission is Mr. Bob Weyant, Director, Internal Review at (703) 553-5627.

MARVIN K. McNAMARA
Brigadier General, USA
Deputy Director

Attachments:
As stated

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates

1	The Ballistic Missile Defense System is comprised of various elements to include the Ground-Based Midcourse Defense (GMD) system. The GMD system is comprised of the following components:
	• GMD Communications Network (GCN);
	• Command Launch Equipment, Fire Control Communications, Ground Based Support, and In-Flight Interceptor Communications Systems; and
	• sensors, radars, and interceptors.
		Concur w/ Comment	"The GMD system is comprised of the following components...." followed by three bullets needs to be re-written for correctness. Change as follows:
			"The GMD system is comprised of the following components:
			   -- Ground-Based Interceptor (GBI)
			   -- Upgraded Early Warning Radars (UEWR)
			   -- Sea-based X-Band Radar (SBX)
			   -- GMD Fire Control and Communications (GFC/C).
			The GFC/C consists of the GMD Fire Control (GFC), GMD Communications Network (GCN), and the In-Flight Interceptor Communication System (IFICS)."
			Estimated Completion Date: N/A

2	MDA officials had not prepared an SSAA for the GCN. Contractor officials did not prepare and update the various GCN components SSAAs to adequately reflect the current operating system mission, environment, and architecture.	Concur w/ Comment	Separate SSAAs for each of the four GCN components (LHC, CNE, LSM, NSM) were created and signed. To comply with the DOD IG recommendation, a single SSAA will be created that includes the GCN components as separate annexes. This will be staffed for signature by the GMD PD. The SSAAs updates also will include the GT04-2A.1 Annex P and Q updates. Estimated Completion Date: 6 Mar 06
3	**Recommendation:** Complete the **System Security Authorization Agreement** process for the Ground-Based Midcourse Defense Communications Network.	Concur w/ Comment	Separate SSAAs for each of the four GCN components (LHC, CNE, LSM, NSM) were created and signed. To comply with the DOD IG recommendation, a single SSAA will be created that includes each of the GCN components as annexes. This will be staffed for signature by the GMD PD. The SSAAs updates also will include the GT04-2A.1 Annex P and Q updates. Estimated Completion Date: 6 Mar 06

Page 1 of 14

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
4	GCN users did not receive **IA awareness training** prior to being granted access to GCN.	Concur w/ Comment	All users have received IA training. Agree contractor access to components was managed at the component level prior to standing up the ISSO positions, and as a consequence, the process was performed differently by multiple contractors. Currently, process uniformity across all components and contractors is in place with respect to approved access, IA training, and audits. MDA IA awareness training policy currently under development. Estimated Completion Date: Complete
5	**IA Awareness Training:** Contractor personnel who had access to the system did not receive **IA awareness training** prior to being granted to the system.	Concur w/ Comment	All users have received IA training. Agree contractor access to components was managed at the component level prior to standing up the ISSO positions, and as a consequence, the process was performed differently by multiple contractors. Currently, process uniformity across all components and contractors is in place with respect to approved access, IA training, and audits. MDA IA awareness training policy currently under development. Estimated Completion Date: Complete
6	**Recommendation:** Maintain the **information assurance training** program for all Missile Defense Agency and contractor personnel associated with the Ground-Based Midcourse Defense Communications Network.	Concur w/ Comment	All users have received IA training. Agree contractor access to components was managed at the component level prior to standing up the ISSO positions, and as a consequence, the process was performed differently by multiple contractors. Currently, process uniformity across all components and contractors is in place with respect to approved access, IA training, and audits. MDA IA awareness training policy currently under development. Estimated Completion Date: Complete

Page 2 of 14

23

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
7	**Contingency and Incident Response Plans** were not prepared.	Concur w/ Comment	Contingency Operations and Incident Response Policies that specifically address IA requirements are included in the pending ECP SOW with the Prime developer. In the interim, Contingency and Incident Response are present at each site and based on the developer's current NOC operations plans and procedures. Policy Estimated Completion Date: 15 Feb 05 Plans Estimated Completion Date: 6 months after Policy is in effect
8	**Contingency Plan:** GMD officials stated that they had not prepared a formal contingency plan for the GCN because redundant operations had been built into the configuration of the system that would mitigate most interruptions.	Concur w/ Comment	Contingency Operations and Incident Response Policies that specifically address IA requirements are included in the pending ECP SOW with the Prime developer. In the interim, Contingency and Incident Response are present at each site and based on the developer's current NOC operations plans and procedures. Policy Estimated Completion Date: 15 Feb 05 Plans Estimated Completion Date: 6 months after Policy is in effect
9	**Incident Response Plan:** Contractor officials did not prepare a formal incident response plan for the GCN system. Contractor officials stated that they report on equipment and communications outages; however, they do not have a formal plan to report security incidents or violations.	Concur w/ Comment	Contingency Operations and Incident Response Policies that specifically address IA requirements are included in the pending ECP SOW with the Prime developer. In the interim, Contingency and Incident Response are present at each site and based on the developer's current NOC operations plans and procedures. Policy Estimated Completion Date: 15 Feb 05 Plans Estimated Completion Date: 6 months after Policy is in effect

Page 3 of 14

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
10	**Recommendation:** Prepare a contingency plan for the Ground-Based Midcourse Defense Communications Network.	Concur w/ Comment	Contingency Operations and Incident Response Policies that specifically address IA requirements are included in the pending ECP SOW with the Prime developer. In the interim, Contingency and Incident Response are present at each site and based on the developer's current NOC operations plans and procedures. Policy Estimated Completion Date: 15 Feb 05 Plans Estimated Completion Date: 6 months after Policy is in effect
11	**Recommendation:** Prepare an incident response plan for the Ground-Based Midcourse Defense Communications Network.	Concur w/ Comment	Contingency Operations and Incident Response Policies are included in the pending ECP SOW with the Prime developer. In the interim, Contingency and Incident Response are present at each site and based on the developer's current NOC operations plans and procedures. Policy Estimated Completion Date: 15 Feb 05 Plans Estimated Completion Date: 6 months after Policy is in effect
12	**User access** procedures and controls were not properly implemented or documented.	Concur w/ Comment	ISSO has procedures to approve access to GMD resources with appropriate data owner, security manager, and ISSO review, and is based on appropriate security clearance and need to know. Access approval forms are being maintained by ISSO. MDA policy for User Access is under development with a projected approval in Jan 06. Estimated Completion Date: Complete
13	Further, a **Plan of Action and Milestones** designed to assist managers in correcting security weaknesses had not been prepared.	Concur w/ Comment	POA&M is complete; however, as recommended, it will be updated to include the DOD IG findings, upon receipt of the final report. Estimated Completion Date: 15 Feb 06

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
	Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)		
14	**Plan of Action and Milestones:** MDA officials did not implement a formal plan that would assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses identified for the GCN, which is operating under an interim authority to operate.	Concur w/ Comment	POA&M is complete. It will be reviewed quarterly to update and include new actions and milestones, such as the DOD IG findings upon receipt of the final report. Estimated Completion Date: Complete
15	**Plan of Action and Milestones:** Although contractor officials routinely assess the GCN to identify IA security weaknesses, the developing contractor and the independent assessment team contractor maintained the results of those assessments separately.	Concur w/ Comment	As part of the government's DITSCAP, assessment of security risk is provided and shared by both Government independent assessment team contractor and Prime and applicable stakeholders who participate in one or more TIMs until all risks are assessed and mitigation is agreed to at time of IATO renewal. Estimated Completion Date: Complete
16	**Recommendation:** Update the Plan of Action and Milestones to include all security weaknesses identified for the Ground-Based Midcourse Defense Communications Network, including all weaknesses identified in this review.	Concur w/ Comment	POA&M is complete. It will be reviewed quarterly to update and include new actions and milestones, such as the DOD IG findings upon receipt of the final report. Estimated Completion Date: Complete
17	**No User Representative** had authorized the GCN documentation.	Non-concur	**Reason for non-concur and proposed alternative action:** User Representative authorized the current GMD Element and BMDS level SSAA documentation. This process was in-place at the time of the audit. Estimated Completion Date: N/A

Page 5 of 14

26

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
18	**Available Security Documentation**: Additionally, the SSAA for the unencrypted communications system stated that an individual password was required; however, the developing contractor stated that a group password was in use.	Concur w/ Comment	Access to LHC components is achieved through the Long-Haul Comm (LHC) System Manager (LSM), for which individual user accounts with secret passwords are implemented for each user. Access to Comm Node Equipment (CNE) components is achieved similarly through the Network System Manager (NSM) where individual user accounts with secret passwords are needed for access to network components. At the time of the IG investigation, multiple users shared the CNE passwords. With release of the CNE/NSM 4B.1 software build, shared passwords have been eliminated. Estimated Completion Date: Complete
19	**Recommendation**: b. Update the Ground-Based Midcourse Defense Communications Network configuration to include: (2) Individual user passwords to access the unencrypted communications system.	Concur	See comments above in #18. Estimated Completion Date: Complete
20	**Information Assurance Controls**: MDA officials had not fully implemented select **IA controls** required to protect the confidentiality, integrity, and availability of the GCN information.	Concur w/ Comment	All communication paths external to protected areas are encrypted using NSA Type-1 approved encryption. Accesses to LHC components on management channels are via encrypted VPN channels. (2) Integrity: Integrity of mission data is accomplished via multiple layers of ack/nak protocols, message integrity validation rules, and encrypted channels. (3) Availability: Availability is accomplished via redundant path communications with dedicated channel design. In the future, IA controls will be implemented via the next IA ECP for the Prime developer to include IA awareness training, intrusion detection, real-time monitoring, and contingency planning. Estimated Completion Date: Complete

Page 6 of 14

27

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
	Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)		
21	**User Access Controls:** MDA and contractor officials did not conduct adequate reviews for potential acts of unauthorized access into the GCN, implement consistent password procedures, or implement procedures to ensure that access was granted only after users received IA awareness training.	Concur w/ Comment	Agree, the developer was not contracted to provide operations support when Testbed assets were initially installed. Dedicated ISSO and Ops support started in 2005, and a temporary ISSO was assigned in Jun 05 until a dedicated ISSO was hired and trained. Currently, all users have received IA training and new users are required to receive IA training prior to being granted access. Estimated Completion Date: Complete
22	**Unauthorized Access Review:** MDA and contractor officials did not conduct audit log reviews for the unencrypted communications and monitoring systems of the GCN. Contractor officials stated that audit log reviews were only required for the encrypted communications and monitoring systems and that those reviews were performed manually. Contractor officials also stated that manual audit log reviews were cumbersome and time-consuming and that those reviews did not guarantee all relevant security violations would be detected.	Concur w/ Comment	Agree, the developer was not contracted to provide operations support when Testbed assets were initially installed. Dedicated ISSO and Ops support started in 2005, and a temporary ISSO was assigned in Jun 05 until a dedicated ISSO was hired and trained. Currently, all users have received IA training and new users are required to receive IA training prior to being granted access. Estimated Completion Date: Complete
23	**Unauthorized Access Review:** Contractor officials stated that they did not implement real-time audit log monitoring capability on the GCN system because it was not in the contract to do so.	Concur w/ Comment	Current equipment is not capable of performing automated audit logging and assessment. Until that capability is available, audit log monitoring is conducted manually. For clarity, the Trusted Computer Base (TCB) does provide near real-time recording of security relevant events in security audit files; however, continuous monitoring of security relevant events is purely an 8500.2 requirement. GMD is performing weekly manual audits as described in comment below. Estimated Completion Date: Complete

Page 7 of 14

28

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
24	**Unauthorized Access Review:** MDA and contractor officials should also conduct weekly manual reviews of the audit logs for all GCN components until such time that an automated monitoring capability is installed into the system.	Concur w/ Comment	GMD ISSOs conduct weekly audits (manually) and report their Findings to the Boeing Weapon System Operational Security Manager. Estimated Completion Date: Complete
25	**Recommendation:** b. Update the Ground-Based Midcourse Defense Communications Network configuration to include: (1) Automated monitoring of the unencrypted and encrypted communications and monitoring systems	Concur w/ Comment	See comments above in #24. Estimated Completion Date: Complete
26	**User Account Management:** Contractor officials explained that based on the configuration of the GCN, an individual password was not necessary to protect against unauthorized use.	Concur w/ Comment	Access to LHC components is achieved through the Long-Haul Comm (LHC) System Manager (LSM), for which individual user accounts with secret passwords are implemented for each user. Access to Comm Node Equipment (CNE) components is achieved similarly through the Network System Manager (NSM) where individual user accounts with secret passwords are needed for access to network components. At the time of the IG investigation, multiple users shared the CNE passwords. With release of the CNE/NSM 4B.1 software build, shared passwords have been eliminated. Estimated Completion Date: Complete

Page 8 of 14

29

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
27	**User Account Management:** DoD policy does not allow for individual or role-based passwords, even when the configuration of the system provides protection against unauthorized access.	Concur w/ Comment	Access to LHC components is achieved through the Long-Haul Comm (LHC) System Manager (LSM), for which individual user accounts with secret passwords are implemented for each user. Access to Comm Node Equipment (CNE) components is achieved similarly through the Network System Manager (NSM) where individual user accounts with secret passwords are needed for access to network components. At the time of the IG investigation, multiple users shared the CNE passwords. With release of the CNE/NSM 4B.1 software build, shared passwords have been eliminated. Estimated Completion Date: Complete
28	**User Account Management:** Contractor officials did not implement a plan or prepare procedures to deactivate inactive, suspended, or terminated accounts promptly.	Concur w/ Comment	ISSO process are currently in place to ensure users accounts (e.g. unused, expired, aged, etc) are suspended are deleted. Estimated Completion Date: Complete
29	**User Account Request Forms:** Fourth, two accounts were still active when those users were no longer at that operating location.	Concur w/ Comment	Processes are implemented to disable accounts of persons who depart (either TDY or PCS) a location. However, it is recognized that, in some cases individuals may still require remote access for maintenance and management from a central location as described above. Estimated Completion Date: Complete
30	**Recommendation:** Immediately implements all information assurance controls required in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, for Mission Assurance Category I and classified systems. Specifically: (1) **Deactivate inactive, suspended, and terminated accounts.**	Concur w/ Comment	Prime Contractor has implemented this process. Estimated Completion Date: Complete

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
31	**User Account Management:** MDA officials should require the contractor to immediately prepare and implement account management procedures to include deactivation of inactive, suspended, or terminated accounts.	Concur w/ Comment	Prime Contractor has implemented this process. Estimated Completion Date: Complete
32	**User Account Request Forms:** However, the GCN IA Officer had not been appointed until June 2005, almost a year after the GCN became operational.	Concur w/ Comment	ISSO position authorized in Jan 05. Temporary ISSO assigned Apr 05. Permanent ISSO hired & assigned in Jun 05. Training began in late Jun 05. Estimated Completion Date: Complete
33	**User Account Request Forms:** For the 22 user account request forms reviewed, the GCN security manager had not signed those forms verifying that a user had the required security clearance for the GCN until July 25, 2005, approximately one year after the GCN became operational.	Concur w/ Comment	ISSO position recently established. User forms were prepared and signed via email. An updated process was identified and was going through approval and signature cycle at time of audit. New form and process are currently in place. Since ISSO establishment at JNIC, a common set of processes and forms for granting access was developed. For each account, a completed User Access Control and Account Creation form is now audited and verified by the ISSO. Estimated Completion Date: Complete
34	**Recommendation:** (2) Mandate that the information assurance officer track the date a user is granted access to the system, certify the user completed information assurance awareness training, and verify that the user has a valid and appropriate security clearance.	Concur w/ Comment	Prime Contractor has implemented this process. Estimated Completion Date: Complete
35	**User Account Request Forms:** First, the system administrator creating accounts on the GCN created his own account and granted himself all levels of access allowed for the GCN.	Concur w/ Comment	System Administrator Resources for NSM and LSM are limited to 1 person per site who are also operators. The System Administrator is responsible for creating all accounts on each system, including their own. Now for each account a completed User Access Control and Account Creation form is audited and verified by the ISSO. Estimated Completion Date: Complete

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
36	**Recommendation:** (3) Require than an independent party validate in the Ground-Based Midcourse Defense Communications Network that access requirements granted were appropriate when a user creates their own account.	Concur w/ Comment	Validation will be performed by the independent C&A Team. A validation process will be added to the ST&E procedures. Estimated Completion Date: Complete
37	**User Account Request Forms:** Second, the revised forms were not completed by the unencrypted communications and monitoring systems users.	Concur w/ Comment	User forms were prepared and signed via email. An updated process was identified and was going through approval and signature cycle at time of audit. New form and process in place. Since ISSO establishment at JNIC, a common set of processes and forms for granting access has been developed. Now for each account a completed User Access Control and Account Creation form is audited and verified by the ISSO. Estimated Completion Date: Complete
38	**User Account Request Forms:** Third, the IA Officer and security manager at one operating location certified IA training requirements and security clearances on the user account access forms for a location they were not responsible for.	Concur w/ Comment	The Prime Contractor and MDA maintain a system-level IA Training matrix that is used across the GMD Program. Certain personnel are certified to perform operations on AIS equipment at multiple sites. Certain individuals are also cross-authorized on systems to allow remote maintenance and system management (without travel). The ISSOs and Security Officers use a common database to verify clearances and IA Training. Estimated Completion Date: Complete
39	**User Account Request Forms:** Lastly, the security manager certified users' clearances a day after our receipt of the revised forms.	Concur w/ Comment	The LSM User Access Control and Account Creation forms were implemented in early November 05, coinciding with the IG Team's request for additional data. The JNIC FSO inadvertently entered the wrong date of her Clearance Check on each of the LSM operator Access Control and Account Creation Forms. Estimated Completion Date: Complete

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
40	**User Account Request Forms:** MDA officials should require the contractor to update and prepare procedures that require the user account request form include the date users are granted initial access to the system in order to track that annual IA refresher training is being provided and require the IA Officer to certify by initialing the form that the:	Concur w/ Comment	The Prime Contractor has fully implemented new User Access Control and Account Creation Forms for GCN. Estimated Completion Date: Complete
41	**User Account Request Forms:** • user had completed the IA awareness training;	Concur w/ Comment	Contained on the User Access Control and Account Creation Form. Documentation is verified by ISSO. Estimated Completion Date: Complete
42	**User Account Request Forms:** • supervisor verified the user's role and need-to-know; and	Concur w/ Comment	Contained on the User Access Control and Account Creation Form. Documentation is verified by Manager. Estimated Completion Date: Complete
43	**User Account Request Forms:** • security manager certified the user holds a valid and appropriate clearance.	Concur w/ Comment	Contained on the User Access Control and Account Creation Form. Documentation is verified by FSO. Estimated Completion Date: Complete

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
44	**Management Controls**: Contractor officials stated that because the GCN had been in development for approximately five years, it would have been too costly to modify the development contract to implement the IA controls required in DoD Instruction 8500.2; however, security requirements cannot simply be waived based on cost.	Concur w/ Comment	Official requirement change to comply with DODI 8500.2 occurred in October 2002 (2 years after GCN was in implementation phase (PDR May 2000). Prime is working with MDA to address risk analysis and capabilities that are required to bring system into full regulatory compliance. In 2003 Prime and Government addressed the delta risk and bridging IA controls. Government intends to put those controls in place via ECP that includes: 1) Network Intrusion Detection System, 2) GMD component implementation of GMD Common Security Configurations and responses to IA Vulnerability Alert/Bulletins, 3) Development and procurement of System Security Management Station (SSMS) Platform 4) Development and procurement of SSMS Application Software, 5) Implementation of Element Interface Boundary Protection (EIBP) devices at GMD enclave and external network boundaries, 6) Implementation of GMD Network Intrusion Detection System (NIDS), 7) Maintenance and Sustainment for IA/CND 8) Information Assurance Operations to include SSMS operator and security management that provides monitoring and reporting. Estimated Completion Date: ECP Projected award date is April 06

<div align="center">Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)</div>

Page 13 of 14

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates

Missile Defense Agency Response to DoD Inspector General Draft Audit Report #D2005-D000AL-0152 on Select Controls for the Information Security of the Ground-based Midcourse Defense Communications Network (GCN)

	DOD Inspector General Draft Report Text	MDA Concur or Non-concur	MDA Actions Taken or Planned and Estimated Completion Dates
45	**Management Controls:** Memorandum, "Mission Assurance Category (MAC) Levels for Missile Defense Agency (MDA) Systems and Networks," August 20, 2004, required that MDA systems and networks not accredited in accordance with DoD Instruction 8500.2 be approved in writing from the MDA Designated Approving Authority; however, no written approval was obtained. Additionally, the MDA CIO stated that although the contractor had not implemented all the IA controls required by DoD Instruction 8500.2, the standards used, DoD 5200.28-STD, met approximately 85 percent of those IA controls. However, that standard is twenty years old and does not include requirements for the current IA controls of DoD Instruction 8500.2.	Concur w/ Comment	The MDA CIO is the signatory DAA for the GMD Element, and he has signed its IATO pending upgrades to DODI 8500. Estimated Completion Date: Complete
46	**Management Controls:** MDA officials had not prepared IA policies for incident response and recovery, passwords, configuration change, IA training, and audit management. MDA officials only first entered into a contract for the development of those IA policies in June 2005, after an assessment of their IA program conducted by the National Security Agency.	Concur w/ Comment	All cited IA Policies currently under development with Task Order 0008, HQ0006-02-C-0002, Active Survivability Enhancement (ASE) Program. Estimated Completion Date: Mar 06
47	**Recommendation:** (2) Mandate that the information assurance officer track the date a user is granted access to the system, certify the user completed information assurance awareness training, and verify that the user has a valid and appropriate security clearance.	Concur w/ Comment	Prime Contractor has implemented this process. Estimated Completion Date: Complete
48	**Recommendation:** Report in the Missile Defense Agency's Annual Statement of Assurance the information assurance weaknesses identified in this report for the Ground-Based Midcourse Defense Communications Network.	Concur w/ Comment	A change to the Report in the Missile Defense Agency's Annual Statement of Assurance will be considered at the annual update. Estimated Completion Date: Mar 06

Page 14 of 14

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Readiness and Logistics Support prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Kathryn M. Truex
Karen J. Lamar
George A. Leighton
Courtney E. Woodruff
Tina N. Brunetti
Dawn M. Russell